A

K M M INSTITUTE OF POSTGRADUATE STUDIES ::TIRUPATI

MCA 305A- CRYPTOGRAPHY AND NETWORK SECURITY

Max Time: 3 hrs **Pre-final examination** **Max. Marks: 100**

Section – A

Answer any FIVE questions, each question carry equal marks **5 x 5 = 25**

1. Differentiate between symmetric and asymmetric cryptosystem
2. Which parameters and design choices determine the actual algorithm of a Fiestel Cipher.
3. Encrypt the message "the house is being sold tonight" using Vigenere cipher with key "dollars". Ignore the space between words. Decrypt the message to get the plain text.
4. Compare stream cipher and block cipher with example.
5. List different types of attacks addressed by message authentication.
6. Illustrate Needham and Schroedor protocol for mutual authentication.
7. Compare transport mode and tunnel mode functionalities in IPSec.
8. List out the five header fields and their meaning defined in MIME.
9. Compare SSL and TLS.
10. Explain Block Chain Technology.

Section – B

Answer any Five questions choosing ONE from each Unit **15 x 5 = 75**

Unit-1

11. a) Discuss about different poly alphabetic cipher substitution techniques.
    b) Explain single round of DES algorithm.
12. a) Differentiate between Confusion and Diffusion.
    b) Explain the key generation in IDEA

Unit-2

13. Explain AES algorithm in detail.
14. a) Explain the algorithm for generating keys in RSA algorithm. Perform encryption and decryption using RSA Alg. for the following.. P=7; q=11; e=13; M=8
    b) Illustrate man in the middle attack on Diffie-Hellman key exchange algorithm

Unit-3

15. a) Explain three different Arbitrated Digital Signature Techniques.
    b) What is suppress replay attack in authentication? Explain the protocol used to eliminate this attack
16. a) Explain the sequence of steps involved in the message generation and reception in PGP with block diagrams.
    b) List out the benefits of IPSec.

Unit-4

17. a) Explain the features of any two types of firewalls.
    b) Explain the sequence of operations required for Secure Electronic Transaction.
18. a) Explain the format of IPSec ESP Packet.
    b) Illustrate the overall operation of SSL Record Protocol.

Unit-5

19. How signing and verification is done in Digital Signature algorithm.
20. Explain Threats & Security in Cloud computing.

B

K M M INSTITUTE OF POSTGRADUATE STUDIES ::TIRUPATI

MCA 305A- CRYPTOGRAPHY AND NETWORK SECURITY

Max Time: 3 hrs **Pre-final examination** **Max. Marks: 100**

Section – A

Answer any FIVE questions, each question carry equal marks **5 x 5 = 25**

1. Explain confusion and diffusion properties of modern block ciphers
2. Differentiate between symmetric and asymmetric cryptosystem
3. Explain the mix column operation in AES algorithm
4. Compute 3^{61} mod 7. use Fermat's Little Theorem
5. What are the requirements of a good hash function?
6. How digital signature is implemented using RSA approach
7. What are the steps for preparing a Signed Data MIME entity?
8. Give the format of Authentication Header in IPSec
9. Explain the handshake protocol in SSL
10. List the various attacks that can be made on packet filtering routers and mention appropriate counter measures

Section – B

Answer any Five questions choosing ONE from each Unit **15 x 5 = 75**

Unit-1

11. a) Give different techniques used in Steganography

b) Explain Block Cipher Design principles and Modes of Operation.

12. a) Explain the S-box design of DES algorithm.

b) Illustrate RC4 algorithm

Unit-2

13 a) Explain the key generation in AES algorithm

b) How round transformation is performed in IDEA

14. Illustrate MD 5 hash algorithm in detail

Unit-3

15. a) Define Euler's Totient Function. Prove that, ϕ(pq) = (p-1)(q-1), where p and q are prime numbers.

b) Demonstrate Diffie Hellman Key exchange algorithm.

16. Explain Conventional Encryption Algorithms: 3 DES, IDEA, Blowfish, RC5.

Unit-4

17. a) Alice and Bob agreed to use RSA algorithm for the secret communication. Alice securely choose two primes, p=5 and q=11 and a secret key d=7. Find the corresponding public key. Bob uses this public key and sends a cipher text 18 to Alice. Find the plain text.

b) State and prove Euler's theorem.

18. a) Explain the method of protecting IP datagram from replay attack using IPsec.

b) Explain the sequence of steps used in Secure Socket Layer handshake Protocol for establishing a new session. Draw a diagram which shows the action of Handshake Protocol.

Unit-5

19. Explain Mobile Security and its Eco System, Service Risks and App Risks.
20. Define Cloud Computing Security, Crypto currency, BitCoin Security and Ethereum.